REMARKS

Applicants respectfully traverse and request reconsideration.

Applicants wish to thank the Examiner for the notice that all of the claims have been allowed except for claims 18-31 and 49.

Claims 18, 19, 20-24 and 27-30 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Appelbaum in view of Auerbach. As to claim 18, in the "Response to Arguments" section of the office action, the responses alleged that Applicants' arguments are against the references only individually. However, Applicants respectfully submit that the references are addressed in combination and that the teachings of each reference must be considered as a whole as required by governing law and as such, selective picking and choosing of teachings of references is improper. In addition, it is respectfully noted that the claim language also cannot be selectively parsed in an effort to eliminate claim limitations or change the meaning of the claims.

In addition, it appears that the "Response to Arguments" section may appear to mischaracterize Applicants' previous remarks. As such, Applicants respectfully reassert the previous remarks. For example, page 2 of the final action states "Applicants' argument that Appelbaum reference does not disclose a first party cryptographic engine is not persuasive because the use of an encryption procedure at a party, which would meet the limitations of a cryptographic engine." However, Applicants specifically state that Appelbaum does not teach the specific type of cryptographic engine as set forth in the claims. Namely one " that produces a double key package wherein the double key package includes a decryption key that is used to decrypt encrypted data that has been encrypted through a double application of an asymmetric public key encryption process." (See Remarks Section, page 14.) In fact, Applicants pointed out

that Appelbaum appears to teach an opposite approach because Appelbaum appears to only describe a symmetric key process that uses a common FK that is used for all computers such that a single fixed key FK is used for all computers and the same encryption procedure is used as set forth, for example, in column 6 of the Appelbaum reference. Since the limitation requires producing a double key package and that double key package includes a decryption key that is used to decrypt encrypted data that has been encrypted through a double application of an asymmetric public key encryption process and since the Appelbaum reference must be read as a whole as understood by one of ordinary skill in the art. The claim limitation is not taught or suggested by Appelbaum. Where one reference teaches a different approach from that claimed, and one of these different approaches is then combined with another reference, the individual teachings of each reference must be understood to determine how a resulting combination of these teachings would be the same or different from Applicants' claimed invention. Since Appelbaum seems to disclose using a single fixed symmetric key to all computers, it teaches a different approach from that claimed by Applicants.

The cited portion of Auerbach being used to reject the claims is the Background of the Invention section of Auerbach. Again, this section appears to teach a single application of an asymmetric encryption whereas the claim requires a different approach, namely a double key package that includes a decryption key that is used to decrypt encrypted data that has been encrypted through a double application of an asymmetric public key encryption process and that it combines a double key package with the cipher text. The office action appears to use the Background of the Invention of Auerbach to teach a complete modification of Appelbaum which allegedly would eliminate the need for the key identifier database of Appelbaum. However, the entire Auerbach reference must be considered. Moreover, there must be some motivation other

than Applicants' own disclosure which would teach a complete redesign of Appelbaum to eliminate the need for a key identifier database as alleged in the office action. Moreover, the combination of the Background of the Invention section of Auerbach with that of Appelbaum would also render Appelbaum's invention unworkable since Appelbaum is dealing with a symmetric key system that uses a key identifier database. Applicants are unable to find any motivation to combine the teachings of Appelbaum and Auerbach.

In fact, the Patent Office does not appear to provide any factual support for any motivation and as such, the rejection does not appear to meet the prima facia requirements of a proper 103 rejection. For example, there is only a conclusory statement that "It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the asymmetric key of Auerbach and the software piracy prevention system of Appelbaum in order to eliminate the need for a key identifier database as taught by Auerbach (column 1, lines 19-25)." There is no indication as to where the motivation comes from to modify the system of Appelbaum nor why one of ordinary skill in the art would do so. The motivation must be set forth in clear terms. Also, Applicants also respectfully request actual support for such motivation as Applicants are unable to find any.

Again, since the cited portion of Auerbach appears to teach a single application of asymmetric encryption and since Appelbaum teaches a different approach using symmetric encryption with a key database, Applicants respectfully submit that the combination of references do not teach or suggest the claimed invention.

The dependent claims add additional novel and non-obvious subject matter. For example, claim 19 requires that the first cryptographic key engine encrypts a first cryptographic key that is used to encrypt the data, with another encryption key that is associated with a second

party. This first key package is then encrypted using a third encryption key associated with a third party to produce the double key package. Again, the use of multiple party keys to generate the double key package as claimed is not taught or suggested in the cited references. Applicants respectfully note that the "allowable subject matter" section of the office action also indicates that the references do not teach encrypting data with a first key and encrypting that key with a second party's key to produce a key package and the encrypting the key package with the third party's encryption key to produce an encrypted key package. Accordingly, this claim is also believed to be in condition for allowance.

Claims 23, 24 and 27 are also believed to be allowable for similar reasons in that the cited references do not teach a double key package that is used to decrypt the encrypted data protected through a double application of an asymmetric public key encryption in combination as claimed. Accordingly, these claims are also believed to be in condition for allowance.

Claims 25, 26 and 31 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Appelbaum in view of Auerbach and in further view of Perlman. Applicants respectfully resubmit the remarks made above and as such these claims are also in condition for allowance.

Claim 49 stands rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 4,712,238 (Gilhousen et al.). The Gilhousen reference appears to be misread. For example, with respect to column 8, the Examiner states on page 4 of the rejection that "Before the channel key is transmitted to the subscriber it is encrypted with a credit signal.". This appears to be incorrect since both FIG. 2 and the cited column 8, lines 39-43 indicate that it is the "category" key signal, not the channel key which is XOR'd with the credit signal. In addition, there does not appear to be a first and second party in the production of a key package as claimed. Column 7, lines 45-60 of Gilhousen describes FIG. 2 as an encryption system of a broadcast terminal and all the data

items comprising an encrypted channel key or an encrypted category key appear to be owned by a single party as outlined in FIG. 2. As such, Applicants respectfully submit that the Gilhousen reference fails to anticipate the claimed subject matter and as such, the claim is in condition for allowance.

Accordingly, Applicants respectfully submit that the claims are in condition for allowance and that a timely Notice of Allowance be issued in this case. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a telephone conference will advance the prosecution of this application.

Respectfully submitted,

Date: 6/21/05

By: _____
Christopher J. Reckamp
Registration No. 34,414

Vedder, Price, Kaufman & Kammholz, P.C.
222 N. LaSalle Street
Chicago, IL 60601
Telephone: (312) 609-7599
Facsimile: (312) 609-5005
Email: creckamp@vedderprice.com